Kiteworks

COMPLIANCE BRIEF

Securing Saudi Financial Institutions

Kiteworks Supports SAMA Cyber Security Framework Compliance

The Saudi Arabian Monetary Authority's (SAMA) Cyber Security Framework, Version 1.0, was released in May 2017. In response to the escalating severity of cyberattacks, the framework aims to assist regulated entities in establishing robust cyber security governance. It underscores the necessity of fortified infrastructure and preemptive measures against cyber threats. The framework's structure encompasses several sections, starting with an emphasis on safeguarding sensitive data and online services within the contemporary digital landscape. Its core objective is to create a unified approach to cyber security while effectively managing the attendant risks. The framework defines cyber security as an amalgamation of tools, policies, safeguards, and technologies designed to safeguard information assets from unauthorized access, alteration, and disruption. It applies across all financial institutions under SAMA's regulation, encompassing banks, insurance companies, financing entities, and credit bureaus. Structured into four core domains—Cyber Security Leadership and Governance, Cyber Security Risk Management and Compliance, Cyber Security Operations and Technology, and Third Party Cyber Security—the framework offers specific principles, objectives, and control considerations for each subdomain.

Overall, the framework underscores the significance of adopting structured approaches to cyber security. It promotes clear policies, standards, and procedures, along with continuous assessment and improvement strategies, as paramount in the management of dynamic cyber threats. The framework's alignment with recognized industry standards such as NIST, ISF, ISO, BASEL, and PCI reinforces its credibility and relevance. Kiteworks offers support to organizations looking to be compliant with this framework. Here's how:

Manage Cyber Security Risk and Compliance

The framework requires cyber security risk response where the cyber security risks of a Member Organization should be treated and where the Member Organization should comply with mandatory international industry standards. Kiteworks helps organizations ensure cyber risks are treated with audit logs and the system dashboard. Within the audit logs, Kiteworks offers complete visibility and control over the communication of IP, PII, PHI, and other sensitive data. This allows organizations to monitor and manage who has access to sensitive information and how it is being used.

Solution Highlights

- **Immutable and consolidated audit logs**
- **AI-powered threat detection**
- **Robust access controls**
- **Centralized third-party communications**
- **Automated workflows**

Additionally, the Kiteworks system dashboard provides a clear and visible system health status. This feature allows administrators to quickly assess the overall health of the system, including server status, network connectivity, and any potential issues that may affect system performance or availability. Audit logs and the system dashboard offer visibility and control to organizations, allowing them to identify and evaluate strengths and weaknesses in their cyber security controls.

Kiteworks provides features that can support organizations in their efforts to comply with the PCI DSS. This includes encryption of data at rest and in transit, access controls, and detailed audit logs. Kiteworks also provides features that can support organizations in their efforts to comply with the SWIFT Customer Security Controls Framework. This includes secure file transfer, encryption of data at rest and in transit, access controls, and detailed audit logs. Kiteworks provides robust security features that can support organizations in their efforts to comply with various security standards and frameworks. It's important to note that compliance is not solely achieved through the use of a particular product or service, but also depends on an organization's broader security practices and procedures.

Safeguard the Protection of the Operations and Technology

To comply with the framework, the Member Organizations have to ensure that security requirements for their information assets and the supporting processes are defined, approved, and implemented. Organizations should incorporate cyber security requirements into human resources processes. It should also define, approve, implement, communicate, and monitor an asset management process, which supports an accurate, up-to-date, and unified asset register, and restrict access to its information assets in line with their business requirements based on the need-to-have or need-to-know principles.

To support Member Organization staff's post-employment cyber security responsibilities, Kiteworks allows administrators to instantly change user access rights post-employment. This can be used to lock down a device or restrict access to sensitive data. To support the Member Organization in having an accurate and up-to-date inventory and central insight in the physical/logical location and relevant details of all available information assets, Kiteworks offers a centralized repository, access controls, life-cycle management, custom reporting, automated workflows, integration, and third-party access. Kiteworks provides a secure, centralized repository to store, categorize, and manage all digital assets and documents, paired with granular access controls to ensure only authorized users can access specific assets based on their role while expiration dates, reviews, and other life-cycle stages can be configured for assets. Then, administrative reports provide visibility into assets, the users accessing them, as well as location and timestamps. Kiteworks strengthens asset management through automated workflows that ensure consistent processes for assets like documents and media files. Tight integration with repositories allows direct management of assets in native systems while controlled third-party access grants external visibility securely. Administrators gain visibility into asset usage across the organization through detailed audit logs and reports. By unifying processes, enabling automation, restricting third-party access, and providing usage transparency, Kiteworks empowers organizations to securely and efficiently manage digital assets across their entire life cycle.

Document and Implement Controls for All Applications

To further comply with the framework to protect the operations and technology, Member Organizations must define, approve, and implement cyber security standards for application systems. Kiteworks provides software hardening, regular penetration testing, quarterly software updates, and compliance reporting to support organizations in their goal to ensure that sufficient cyber security controls are formally documented and implemented for all applications. Kiteworks provides robust application security through a built-in network firewall, web application firewall, and intrusion detection system in its virtual appliance. The platform undergoes regular penetration tests to identify and fix vulnerabilities proactively. One-click appliance updates enable administrators to easily patch the system against the latest threats. Compliance reporting highlights discrepancies, providing information needed for audits to meet regulatory obligations. These capabilities allow Kiteworks to harden the software and help organizations strengthen application security.

Ensure That Access to and Integrity of Sensitive Information Is Protected

Member Organizations should also use cryptographic solutions to ensure that access to and integrity of sensitive information is protected and the originator of communications or transactions can be confirmed. Kiteworks leverages AES-256-bit encryption, the globally recognized standard, to secure all user data. Transmission is protected through SSL encrypted connections between user devices and Kiteworks servers. For an additional level of assurance, Kiteworks offers FIPS 140-3 validated encryption that has passed rigorous U.S. government standards. The platform further safeguards data by encrypting it at rest on Kiteworks servers. Customers can enable key rotation under their control to regularly change encryption keys for stronger security. By encrypting data both in transit and at rest with stringent algorithms, Kiteworks guarantees the confidentiality and integrity of sensitive data. Robust access controls like SSO, 2FA, and granular permission policies ensure only authorized users can access protected data. Detailed audit logs provide accountability by recording user activities for forensics. Taken together, Kiteworks' defense-in-depth encryption, access controls, and activity logging ensure protected access and confirmability of origin for sensitive data communications and transactions.

Protect Personal Devices During Transmission and Storage

Additionally, the framework requires that when Member Organizations allow the use of personal devices for business purposes, the use should be supported by a defined, approved, and implemented cyber security standard, additional staff agreements, and cyber security awareness training. The Kiteworks mobile app enables secure handling of sensitive data on personal mobile devices. All files stored in the app are automatically encrypted, ensuring protection if devices are lost or stolen. Users can reliably access files offline when internet connectivity is limited. For additional security, administrators can remotely wipe app data on compromised devices to prevent data leakage. Secure collaboration is facilitated through controlled file sharing from the app with both internal team members and external partners. Granular permissions provide an additional layer of control over document access. Combined with capabilities like authentication and device management, Kiteworks enables organizations to securely support BYOD programs without compromising security of sensitive business information. The layered protections around encryption, remote wipe, and privileged file sharing allow staff mobility while also ensuring corporate data remains protected on personal devices.

Identify and Respond to Anomalies and Incidents While Understanding Threat Posture

According to the framework, the Member Organization should define, approve, and implement a security event management process to analyze operational and security loggings and respond to security events; define, approve, and implement a cyber security incident management process that is aligned with the enterprise incident management process, to identify, respond to, and recover from cyber security incidents; and define, approve, and implement a threat intelligence management process to identify, assess, and understand threats to the Member Organization information assets, using multiple reliable sources. Kiteworks provides immutable and unified audit logs that record all user and system activities across communication channels. These can be used for administrative tracking, compliance reporting, and end-user transparency. AI-powered alerts notify administrators of potential threats based on suspicious behaviors. The CISO Dashboard leverages analytics to visualize anomalies in user activities, traffic patterns, and file actions for investigation. Robust access controls and least-privilege principles further safeguard data. Tight SIEM integrations enable monitoring of Kiteworks events as part of overall security operations. With proactive threat detection, unified activity trails, visual forensics, and SIEM ingestion, Kiteworks strengthens an organization's security posture. It provides the capabilities to log events, detect incidents, understand threats, and respond effectively. This supports compliance with SAMA requirements for security event, incident, and threat management processes.

Safeguard Third-party Connections With Consolidation and Control of Communications

Cyber security requirements between the Member Organization and third parties should be organized, implemented, and monitored. Kiteworks enables consolidation and control of all external communications across email, file sharing, managed file transfer, mobile apps, web forms, chat, and other channels. All third-party interactions route through the Kiteworks Private Data Network to maintain security. Organizations gain visibility into data accessed in on-premises or cloud repositories that is shared externally.

Granular policies, ethical walls, and encryption applied by Kiteworks ensure sensitive data remains protected when engaging third parties. Support for robust integrations allows extending capabilities to address unique needs. With unified communication oversight, content-aware controls, and adaptive integrations, Kiteworks provides the capabilities to organize, implement, monitor, and demonstrate compliance with cyber security requirements around third-party interactions. This aids adherence to SAMA's stipulations for managing and securing external connections.

The Saudi Arabian Monetary Authority's Cyber Security Framework delivers prescriptive guidance to safeguard information assets against escalating cyber threats. It advocates structured policies, continuous assessments, and industry alignment to manage risks dynamically. Kiteworks' unified controls, proactive threat detection, access safeguards, and consolidated auditing empower financial institutions to realize the framework's objectives. The platform enables progressive security event, incident response, and threat management per SAMA directives. It also facilitates compliance with standards like PCI DSS for robust infrastructure protection. With its defense-in-depth approach across encryption, logging, analytics, permissions, and third-party oversight, Kiteworks provides a powerful means to fulfill SAMA requirements while advancing cyber resilience. Financial organizations can leverage Kiteworks as a critical component of their cyber security programs, harnessing its capabilities to securely enable digital processes and uphold customer trust. Taken together, Kiteworks' multifaceted protections and compliance-centric features allow regulated entities to adopt SAMA standards effectively.